(iii) creating a second signature comprising a plurality of parameters related to the transmission of messages over a second period shorter than the first and more recent than the first;

[(iii)](iv) updating the first signature by a weighted averaging with the second signature;

([i]v) detecting anomalies by inputting the signatures to the anomaly detector; and

[(v)](vi) processing the signatures using the anomaly detector to derive the anomalies by detecting unexpected patterns in the transmission of messages by the entity over the time period.

---

10. (thrice amended) The method of Claim 1 wherein said step (vi) of processing the signatures is carried out using a predictive model, the method further comprising the steps of:

monitoring the performance of the model; and

automatically updating the model when the performance reaches a predetermined threshold.

11. (thrice amended) The method of Claim 1 wherein said step (vi) of processing the signatures is carried out using a predictive model, and wherein the model is implemented using at least one instantiated object created using an object oriented programming language and the method further comprises the steps of:

converting the object into a data structure;

storing the data structure; and

recreating the object from the data structure.

12. (thrice amended) A computer system for detecting anomalies in [the transmission of] messages transmitted by an entity [by storing information relating to the transmission of messages by the entity over a given time period said computer system] comprising:

(i) a data store arranged to store information relating to the transmission of messages by the entity over a given time period,

(ii) an input arranged to receive information about each of a number of events which occurred during the time period;

(iii) a processor arranged to convert the information into a signature comprising a plurality of parameters related to the transmission of messages over the time period wherein the parameters comprise at least one parameter related to the transmission of messages over a portion of the period and also related to the position of the portion in the period, to enable output data to be derived from the stored information and wherein said processor is further arranged to convert at least part of the information

into a second signature, comprising a plurality of parameters related to the transmission of messages over a second period, shorter than the first and more recent than the first; and also to update the first signature by a weighted averaging with the second signature;

[(iii)](iv) an anomaly detector;

([i]v) an input arranged to provide the signatures to the anomaly detector; [and wherein] the anomaly detector [is] being arranged to process the signatures to derive the anomalies by detecting unexpected patterns in the transmission of messages by the entity over the time period.

13. (thrice amended) A method of deriving anomalies from [information relating to the transmission of] messages transmitted by an entity over time, [using an anomaly detector and] comprising the steps of:

(i) creating a first signature comprising a plurality of parameters related to the transmission of messages over a predetermined first time period;

(ii) creating a second signature comprising a plurality of parameters related to the transmission of messages over a second period shorter than the first and more recent than the first;

(iii) updating the first signature by a weighted averaging with the second signature;

(iv) inputting the signatures to the anomaly detector; and

(v) detecting anomalies by processing the signatures using the anomaly detector to derive the anomalies by detecting unexpected patterns in the transmission of messages by the entity over the time period.

---

22. (thrice amended) A computer system for [deriving] detecting anomalies [from] in [information relating to the transmission of] messages transmitted by an entity over time, the system comprising:

an input arranged to receive information about the transmission of messages by the entity;

a processor arranged to create a first signature comprising a plurality of parameters related to the transmission of messages over a predetermined first time period and to create a second signature comprising a plurality of parameters related to the transmission of messages over a second period shorter than the first and more recent than the first;

a processor arranged to calculate a weighted averaging of the first and second signatures to form an updated first signature;

an anomaly detector;

an input arranged to provide the signatures to the anomaly detector; and

wherein said anomaly detector is arranged to process the signatures to derive the anomalies by detecting unexpected patterns in the transmission of message by the entity over the time period.

---

23. (amended) A method of [deriving] detecting potentially fraudulent telephone calls in [from] information relating to telephone calls associated with an entity over a given time period [and using an anomaly detector], said method comprising the steps of:

(i) creating a first signature comprising a plurality of parameters related to the associated telephone calls over that time period;

(ii) creating a second signature comprising a plurality of parameters related to the associated telephone calls over a second period shorter than the first and more recent that the first;

(iii) updating the first signature by a weighted averaging with the second signature;

(iv) inputting the signatures to the anomaly detector; and

(v) detecting anomalies by processing the signatures using the anomaly detector to [derive] detect the potentially fraudulent telephone calls by detecting unexpected patterns in the telephone calls associated with the entity over the time period.

---

29. A computer system for detecting potentially fraudulent telephone calls [from] in telephone calls associated with an entity over time, the system comprising:

(i) an input arranged to receive information about the telephone calls associated with the entity;

(ii) a processor arranged to create a first signature comprising a plurality of parameters related to the telephone calls over a predetermined first time period and to create a second signature comprising a plurality of parameters related to the telephone calls over a second period shorter than the first and more recent than the first; and wherein the processor is arranged to calculate a weighted averaging of the first and second signatures to form an updated first signature;

(iii) an anomaly detector;

(iv) an input arranged to provide the signatures to the anomaly detector; and wherein said anomaly detector is arranged to process the signatures to derive the potentially fraudulent telephone calls by detecting unexpected patterns in the telephone calls associated with the entity over the predetermined time period.

Please add new claims 30-45 as set out below:

---

30. A method of detecting anomalous usage of a network comprising:-

(i) monitoring traffic flowing in the network,

(ii) generating a normal historic signature and a stored historic signature each representative of network usage over a first time period,

(iii) generating a current signature representative of network usage over a second time period which is shorter and more recent than the first time period,

(iv) determining whether the current signature represents normal usage by comparing it with the normal historic signature,

(iv) if the current signature is determined to represent normal usage, producing an updated stored historic signature by combining the stored historic signature and the current signature using a weighted averaging procedure so that consistent trends present in the current signature are gradually over time introduced into the longer term trends incorporated in the stored historic signature,

(vi) providing an indication of anomalous network usage if the present usage as represented by the current signature deviates from that represented by the normal historic signature by more than a predetermined amount.

31. A method according to claim 30, further comprising receiving validation data which indicates for each second time period whether the usage was, in fact, anomalous and comparing the anomaly indications provided under step (vi) above with the validation data and thereby generating an accuracy measure which represents the accuracy of the anomaly indications.

32. A method according to claim 31 wherein when the accuracy measure indicates an accuracy below a predetermined threshold, the historic signature is replaced with the stored historic signature

33. A method according to 32, wherein the anomaly indication is provided by a neural network and wherein the replacement of the historic signature with the stored historic signature is carried out by re-training the neural network.

34. A method according to claim 30, wherein the network is a telecommunications network and the traffic flowing in the network is selected form the group of voice and data traffic.

35. A method according to claim 30, wherein the network is a cellular mobile telecommunications network and the traffic flowing in the network includes traffic flowing between a mobile station and a base station forming part of the network.

36. A method according to claim 30, wherein the current, historic and stored historic signatures are generated by parsing and analysing call data records (CDR) in a telecommunications network.

37. A method according to claim 30, wherein each current signature and each historic signature is associated with an individual network user.

38. A method according to claim 30, comprising training a neural network to recognise the difference between current signatures which represent normal and anomalous usage of the network.

39. A method according to claim 30, wherein the step of comparing present usage with the current and historic signatures is carried out by at least one pre-trained neural network.

40. Apparatus for detecting anomalous usage of a network comprising:-

(i) a traffic data input arranged to receive traffic data representative of traffic flowing in the network,

(ii) a historic signature generator arranged to process the traffic data and to generate a normal historic signature and a stored historic signature each representative of network usage over a first time period,

(iii) a current signature generator arranged to process the traffic data to generate a current signature representative of network usage over a second time period which is shorter and more recent than the first time period,

(iv) an anomaly detector arranged to determine whether the current signature represents normal usage by comparing it with the normal historic signature and further arranged to produce an updated stored historic signature by combining the stored historic signature and the current signature using a weighted averaging procedure so that consistent trends present in the current signature are gradually over time introduced into the longer term trends incorporated in the stored historic signature, if the current signature is determined to represent normal usage, and

(v) an anomaly output arranged to provide an indication of anomalous network usage if the anomaly detector determines that present network usage as represented by the current signature deviates from that represented by the normal historic signature by more than a predetermined amount.

41. Apparatus to claim 40, further comprising a validator arranged to receive validation data which indicates for each second time period whether the usage was, in fact, anomalous arranged to compare the anomaly indications provided via the anomaly output with the validation data and to generate an accuracy measure which represents the accuracy of the anomaly indications.

42. Apparatus according to claim 41 wherein the validator is arranged to cause the anomaly detector to replace the historic signature with the stored historic signature when the accuracy measure indicates an accuracy below a predetermined threshold.

43. Apparatus according to 42, wherein the anomaly detector includes a neural network and wherein the replacement of the historic signature with the stored historic signature is carried out by re-training the neural network.

44. A method according to claim 40, wherein the traffic data are call data records (CDR) in a telecommunications network.

45. A method according to claim 40, wherein the historic and current signature generators are arranged to associate each respective current signature and historic signature with an individual network user.

Remarks

The Examiner's detailed analysis of the claims is noted and appreciated.

Claim Rejections under 35 USC § 103

The Examiner has rejected all the pending claims as being obvious in view of Hunt and Gillick.